CLAIMS

1. A system for providing secure communication of messages between a mobile node and a home domain using a foreign domain, comprising:

means for transmitting a registration request from the mobile node to the home domain, the request comprising an identity of the mobile node and user in encrypted form and network routing information in non-encrypted form;

means for processing the registration request from the mobile node within the home domain and generating a registration reply comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node, home domain, and the foreign domain; and

means for transmitting the registration reply from the home domain to the foreign domain and the mobile node.

2. The system of claim 1, wherein the means for transmitting a registration request from the mobile node to the home domain comprises:

means for transmitting the registration request from the mobile node to the foreign domain; and

means for transmitting the registration request from the foreign domain to the home domain.

3. The system of claim 2, wherein the means for transmitting the registration request from the foreign domain to the home domain comprises means for establishing a secure communications pathway between the foreign domain and the home domain.

4. The system of claim 2, wherein the means for transmitting the registration request from the foreign domain to the home domain comprises means for establishing a secure communications pathway between the foreign domain and the mobile node.

5. The system of claim 2, wherein the means for transmitting the registration request from the foreign domain to the home domain comprises means for establishing a secure communications pathway between the home domain and the mobile node.

6. The system of claim 1, wherein the means for processing the registration request from the mobile node within the home domain comprises means for decrypting the encrypted form of the identity of the mobile node and user.

7. The system of claim 1, wherein the means for generating a registration reply comprises means for encrypting at least one of the encryption keys.

8. The system of claim 7, wherein the means for generating a registration reply comprises means for encrypting the encryption keys for encrypting messages to be communicated between the mobile node and the home domain, and between the mobile node and the foreign domain.

9. The system of claim 7, further comprising:
means for decrypting one or more of the encrypted encryption keys.

10. The system of claim 1, wherein the means for generating the registration reply comprises:
means for generating a first encryption key for encrypting messages to be communicated between the mobile node and the home domain;
means for generating a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain; and
means for generating a third encryption key for encrypting messages to be communicated between the foreign domain and the mobile node.

11. The system of claim 10, wherein the means for generating the registration reply comprises means for encrypting at least one of the first and third encryption keys.

12. The system of claim 11, further comprising:
means for decrypting at least one of the encrypted first and third encryption keys.

13. The system of claim 1, wherein the registration reply includes:
encryption keys that are encrypted; and
encryption keys that are not encrypted.

14. The system of claim 13, further including:
means for extracting one or more of the encryption keys that are not encrypted from the registration reply.

15. The system of claim 13, further including:
means for extracting and decrypting one or more of the encryption keys that are encrypted from the registration reply.

16. A method of providing secure communication between a mobile node and a home domain using a foreign domain, comprising:
transmitting a registration message from the mobile node to the home domain, the message comprising an identity of a user of the mobile node in encrypted form and network routing information in non-encrypted form;
the home domain receiving and processing the registration message to generate a registration reply comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node, home domain, and the foreign domain; and
transmitting the registration reply from the home domain to the foreign domain and the mobile node.

17. The method of claim 16, wherein transmitting a registration request from the mobile node to the home domain comprises:

transmitting the registration request from the mobile node to the foreign domain; and

transmitting the registration request from the foreign domain to the home domain.

18. The method of claim 17, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the foreign domain and the home domain.

19. The method of claim 17, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the foreign domain and the mobile node.

20. The method of claim 17, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the home domain and the mobile node.

21. The method of claim 16, wherein processing the registration request from the mobile node within the home domain comprises decrypting the encrypted form of the identity of the user.

22. The method of claim 16, wherein generating a registration reply comprises encrypting at least one of the encryption keys.

23. The method of claim 22, wherein generating a registration reply comprises encrypting the encryption keys for encrypting messages to be communicated between the mobile node and the home domain, and between the mobile node and the foreign domain.

24. The method of claim 22, further comprising:

decrypting one or more of the encrypted encryption keys.

25. The method of claim 16, wherein generating the registration reply comprises:

generating a first encryption key for encrypting messages to be communicated between the mobile node and the home domain;

generating a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain; and

generating a third encryption key for encrypting messages to be communicated between the foreign domain and the mobile node.

26. The method of claim 22, wherein generating the registration reply comprises encrypting at least one of the first and third encryption keys.

27. The method of claim 26, further comprising:

decrypting at least one of the encrypted first and third encryption keys.

28. The method of claim 16, wherein the registration reply includes:

encryption keys that are encrypted; and

encryption keys that are not encrypted.

29. The method of claim 28, further including:

extracting one or more of the encryption keys that are not encrypted from the registration reply.

30. The method of claim 28, further including:

extracting and decrypting one or more of the encryption keys that are encrypted from the registration reply.

31. A communications network, comprising:

a home domain;

a foreign domain operably coupled to the home domain; and

a mobile node operably coupled to the foreign domain;

wherein the mobile node is adapted to generate and transmit a registration request to the foreign domain, the registration request including an identity of the mobile node in encrypted form and network routing information in non-encrypted form;

wherein the foreign domain is adapted to relay the registration request to the home domain; and

wherein the home domain is adapted to receive the registration request and generate encryption keys for encrypting messages to be communicated between and among the home domain, the foreign domain, and the mobile node.

32. The network of claim 31, wherein the foreign domain and the home domain are adapted to establish a secure communications pathway between the foreign domain and the home domain.

33. The network of claim 31, wherein the home domain is adapted to decode the encrypted form of the identity of the mobile node.

34. The network of claim 31, wherein the home domain is adapted to encrypt at least one of the encryption keys.

35. The network of claim 34, wherein the home domain is adapted to encrypt the encryption keys for encrypting messages to be communicated between the mobile node and the home domain, and between the mobile node and the foreign domain.

36. The network of claim 34, wherein the mobile node is adapted to decode one or more of the encrypted encryption keys.

37. The network of claim 31, wherein the home domain is adapted to generate:

a first encryption key for encrypting messages to be communicated between the mobile node and the home domain;

a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain; and

a third encryption key for encrypting messages to be communicated between the foreign domain and the mobile node.

38. The network of claim 37, wherein the home domain is adapted to encrypt at least one of the first and third encryption keys.

39. The network of claim 38, wherein the mobile node is adapted to decode at least one of the encrypted first and third encryption keys.

40. The network of claim 31, wherein the home domain comprises:

a home agent operably coupled to the foreign agent; and

an encryption key distribution center operably coupled to the home agent;

wherein the encryption key distribution center is adapted to generate the encryption keys.

41. The network of claim 40, wherein the home domain further comprises:

a home server operably coupled to the home agent; and

wherein the foreign domain comprises:

a foreign agent operably coupled to the home agent and the mobile node; and

a foreign server operably coupled to the foreign agent and the home server.

42. The network of claim 31, wherein the registration reply includes:

encryption keys that are encrypted; and

encryption keys that are not encrypted.

43. The network of claim 42, wherein the foreign domain is adapted to extract one or more of the encryption keys that are not encrypted from the registration reply.

44. The network of claim 42, wherein the mobile node is adapted to extract and decode one or more of the encryption keys that are encrypted from the registration reply.

45. A method of providing secure communications between a mobile node and a home domain using a foreign domain in a communications network, comprising:

the home domain authenticating the mobile node and the foreign domain; and

transmitting messages between the mobile node and the home domain through the foreign domain.

46. The method of claim 45, wherein the home domain authenticates the mobile node and the foreign domain during an initialization process.

47. A registration request message for use in registering a mobile node and a foreign domain with a home domain in a communications network, comprising:

a network address for the home domain; and

a network address for the mobile node;

wherein the home domain and the mobile node share an encryption key for encrypting messages; and

wherein the network address for the mobile node is encrypted using the shared encryption key.

48. A registration reply message for use in registering a mobile node and a foreign domain with a home domain in a communications network, comprising:

encryption keys for encrypting messages to be communicated between and among the mobile node, the home domain, and the foreign domain;

wherein the mobile node and the home domain share an encryption key for encrypting messages; and

wherein the encryption keys for encrypting messages to be communicated between the mobile node and one or more of the home domain and the foreign domain are encrypted using the shared encryption key.

49. A computer program for implementing a method of providing secure communication between a mobile node and a home domain using a foreign domain, comprising:

a storage medium; and

instructions stored in the storage medium for:

transmitting a registration message from the mobile node to the home domain, the message comprising an identity of a user of the mobile node in encrypted form and network routing information in non-encrypted form;

the home domain receiving and processing the registration message to generate a registration reply comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node, home domain, and the foreign domain; and

transmitting the registration reply from the home domain to the foreign domain and the mobile node.

50. The computer program of claim 49, wherein transmitting a registration request from the mobile node to the home domain comprises:

transmitting the registration request from the mobile node to the foreign node; and

transmitting the registration request from the foreign domain to the home domain.

51. The computer program of claim 50, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a

secure communications pathway between the foreign domain and the home domain.

52. The computer program of claim 50, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the foreign domain and the mobile node.

53. The computer program of claim 50, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the home domain and the mobile node.

54. The computer program of claim 49, wherein processing the registration request from the mobile node within the home domain comprises decrypting the encrypted form of the identity of the user.

55. The computer program of claim 49, wherein generating a registration reply comprises encrypting at least one of the encryption keys.

56. The computer program of claim 49, wherein generating a registration reply comprises encrypting the encryption keys for decrypting messages between the mobile node and the home domain, and between the mobile node and the foreign domain.

57. The computer program of claim 55, further including instructions for:
decrypting one or more of the encrypted encryption keys.

58. The computer program of claim 49, wherein generating the registration reply comprises:
generating a first encryption key for encrypting messages to be communicated between the mobile node and the home domain;

generating a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain; and

generating a third encryption key for encrypting messages to be communicated between the foreign domain and the mobile node.

59. The computer program of claim 58, wherein generating the registration reply comprises encrypting at least one of the first and third encryption keys.

60. The computer program of claim 59, further comprising instructions for:

decrypting at least one of the encrypted first and third encryption keys.

61. The computer program of claim 49, wherein the registration reply includes:

encryption keys that are encrypted; and

encryption keys that are not encrypted.

62. The computer program of claim 61, further including instructions for:

extracting one or more of the encryption keys that are not encrypted from the registration reply.

63. The computer program of claim 61, further including instructions for:

extracting and decrypting one or more of the encryption keys that are encrypted from the registration reply.

64. A communications network, comprising:

an initiator;

a responder; and

means for dynamically establishing a security association between the initiator and the responder.

65. The network of claim 64, wherein the means for establishing a security association between the initiator and the responder comprises:

means for negotiating the security association.

66. The network of claim 65, wherein the means for negotiating the security association comprises:

means for negotiating one or more security transforms to be used to provide secure communications between the initiator and the responder.

67. The network of claim 65, wherein the means for negotiating the security association comprises:

means for proposing the number of transforms to be used to provide secure communications between the initiator and the responder.

68. The network of claim 65, wherein the means for negotiating the security association comprises:

means for proposing the duration of at least a portion of the security association.

69. The network of claim 65, wherein the means for negotiating the security association comprises:

means for proposing the type of transforms to be used to provide secure communications between the initiator and the responder.

70. A method of providing secure communications between an initiator and a responder in a communications network, comprising:

dynamically establishing a security association between the initiator and the responder.

71. The method of claim 70, further comprising:

negotiating the security association.

72. The method of claim 71, wherein negotiating the security association comprises:

negotiating one or more security transforms to be used to provide secure communications between the initiator and the responder.

73. The method of claim 71, wherein negotiating the security association comprises:

proposing the number of transforms to be used to provide secure communications between the initiator and the responder.

74. The method of claim 71, wherein negotiating the security association comprises:

proposing the duration of at least a portion of the security association.

75. The method of claim 71, wherein negotiating the security association comprises:

proposing the type of transforms to be used to provide secure communications between the initiator and the responder.

76. A computer program for providing secure communications between an initiator and a responder in a communications network, comprising:

a storage medium; and

instructions recorded in the storage medium for:

dynamically establishing a security association between the initiator and the responder.

77. The computer program of claim 76, further comprising instructions for:

negotiating the security association.

78. The computer program of claim 77, wherein negotiating the security association comprises:

negotiating one or more security transforms to be used to provide secure communications between the initiator and the responder.

79. The computer program of claim 77, wherein negotiating the security association comprises:

proposing the number of transforms to be used to provide secure communications between the initiator and the responder.

80. The computer program of claim 77, wherein negotiating the security association comprises:

proposing the duration of at least a portion of the security association.

81. The computer program of claim 77, wherein negotiating the security association comprises:

proposing the type of transforms to be used to provide secure communications between the initiator and the responder.

82. A communications network, comprising:

an initiator; and

a responder operably coupled to the initiator;

wherein the initiator and the responder are adapted to dynamically establish a security association.

83. The network of claim 82, wherein establishing the security association between the initiator and the responder comprises:

negotiating the security association.

84. The network of claim 83, wherein negotiating the security association comprises:

negotiating one or more security transforms to be used to provide secure communications between the initiator and the responder.

85. The network of claim 83, wherein negotiating the security association comprises:

proposing the number of transforms to be used to provide secure communications between the initiator and the responder.

86. The network of claim 83, wherein negotiating the security association comprises:

proposing the duration of at least a portion of the security association.

87. The network of claim 83, wherein negotiating the security association comprises:

proposing the type of transforms to be used to provide secure communications between the initiator and the responder

88. A protocol extension message for negotiating a security association between an initiator and a responder in a communications network, comprising:

a security association payload for negotiating the security association;

one or more proposal payloads for defining the security association including one or more transforms;

one or more transform payloads associated with each of the proposal payloads for defining the transforms; and

one or more key exchange payloads for defining encryption keys used in the transforms.

89. The protocol extension message of claim 88, wherein the security association payload comprises:

an identification of the entities for the security association.

90. The protocol extension of claim 89, wherein the entities include:

a mobile node and a home agent.

91. The protocol extension of claim 89, wherein the entities include:

a mobile node and a foreign agent.

92. The protocol extension of claim 89, wherein the entities include:

a foreign agent and a home agent.

93. The protocol extension message of claim 88, wherein the proposal payload comprises:

an identification of the duration of the security association.

94. The protocol extension message of claim 88, wherein the transform payload comprises:

an identification of a number of encryption keys required for the transform.

95. The protocol extension message of claim 88, wherein the key exchange payload comprises:

an encryption key for one of the transforms.

96. The protocol extension message of claim 88, wherein the key exchange payload comprises:

a prime number for generating an encryption key;

a generator for generating the encryption key; and

a computed value for generating the encryption key.

97. The protocol extension message of claim 88, wherein the key exchange payload comprises:

an encrypted encryption key for one of the transforms.

98. A method of providing an encryption key for securing communications between an initiator and a responder in a communications network, comprising:

the initiator generating an initiator Diffie-Hellman computed value;

the initiator transmitting the initiator Diffie-Hellman computed value to the responder;

the responder generating the encryption key and a responder Diffie-Hellman computed value;

the responder transmitting the responder Diffie-Hellman computed value to the initiator; and

the initiator generating the encryption key.

99. A method of providing encryption keys for use in securing communications between an initiator and a responder in a communications network, comprising:

providing a predefined shared secret to the initiator and responder;

generating an encryption key for securing communications between the initiator and responder;

encrypting the encryption key for securing communications between the initiator and responder using the predefined shared secret; and

transmitting the encrypted encryption key for securing communications between the initiator and responder to the initiator and responder.

100. A method of generating an encryption key for use in securing communications between an initiator and a responder in a communications network, comprising:

generating an initial encryption key; and

generating an encryption key for securing communications between the initiator and the responder as a pseudo random function of the initial encryption key.

101. The method of claim 100, wherein generating the encryption key for securing communications between the initiator and the responder, further comprises:

generating the encryption key as a pseudo random function of a network access identifier of one or more of the initiator and responder.

102. The method of claim 100, wherein generating the encryption key for securing communications between the initiator and the responder, further comprises:

generating the encryption key as a pseudo random function of an IP address of one or more of the initiator and responder.

103. A communications network; comprising:

an encryption key distribution center for generating an initial encryption key;

an initiator operably coupled to the encryption key distribution center; and

a responder operably coupled to the initiator;

wherein an encryption key for securing communications between the initiator and the responder is generated by one of the key distribution center, initiator, or responder as a pseudo random function of the initial encryption key.

104. The network of claim 103, wherein generating the encryption key for securing communications between the initiator and the responder, further comprises:

generating the encryption key as a pseudo random function of a network access identifier of one or more of the initiator and responder.

105. The network of claim 103, wherein generating the encryption key for securing communications between the initiator and the responder, further comprises:

generating the encryption key as a pseudo random function of an IP address of one or more of the initiator and responder.

106. A communications network; comprising:

means for generating an initial encryption key;

an initiator operably coupled to the means for generating the initial encryption key;

a responder operably coupled to the initiator; and

means for generating an encryption key for securing communications between the initiator and the responder as a pseudo random function of the initial encryption key.

107. The network of claim 106, wherein the means for generating the encryption key for securing communications between the initiator and the responder, further comprises:

means for generating the encryption key as a pseudo random function of a network access identifier of one or more of the initiator and responder.

108. The network of claim 106, wherein the means for generating the encryption key for securing communications between the initiator and the responder, further comprises:

means for generating the encryption key as a pseudo random function of an IP address of one or more of the initiator and responder.

109. A computer program for generating an encryption key for use in securing communications between an initiator and a responder in a communications network, comprising:

a storage medium; and

instructions stored in the storage medium for:

generating an initial encryption key; and

generating an encryption key for securing communications between the initiator and the responder as a pseudo random function of the initial encryption key.

110. The computer program of claim 109, wherein generating the encryption key for securing communications between the initiator and the responder, further comprises:

generating the encryption key as a pseudo random function of a network access identifier of one or more of the initiator and responder.

111. The computer program of claim 109, wherein generating the encryption key for securing communications between the initiator and the responder, further comprises:

generating the encryption key as a pseudo random function of an IP address of one or more of the initiator and responder.

112. A method of establishing a security association between an initiator and a responder in a communication network, comprising:
the initiator proposing a security association; and
the responder responding the proposal.

113. The method of claim 112, wherein the security association comprises:
one or more security protocols.

114. The method of claim 113, wherein at least a portion of the security protocols are combined.

115. The method of claim 112, wherein the security association comprises:
one or more alternative security protocols.

116. A communication network, comprising:
an initiator;
a responder operably coupled to the initiator;
means for proposing a security association between the initiator and the responder; and
means for responding to the proposed security association.

117. The network of claim 116, wherein the security association comprises:
one or more security protocols.

118. The network of claim 116, wherein at least a portion of the security protocols are combined.

119. The network of claim 116, wherein the security association comprises:
one or more alternative security protocols.

120. A communication network, comprising:
an initiator;
a responder operably coupled to the initiator;
wherein the initiator is adapted to propose a security association between the initiator and the responder; and
wherein the responder is adapted to respond to the proposed security association.

121. The network of claim 120, wherein the security association comprises:
one or more security protocols.

122. The network of claim 120, wherein at least a portion of the security protocols are combined.

123. The network of claim 120, wherein the security association comprises:
one or more alternative security protocols.

124. A computer program for establishing a security association between an initiator and a responder in a communication network, comprising:
a storage medium; and
instructions recorded in the storage medium for:
the initiator proposing a security association; and
the responder responding the proposal.

125. The computer program of claim 124, wherein the security association comprises:
one or more security protocols.

126. The computer program of claim 124, wherein at least a portion of the security protocols are combined.

127. The computer program of claim 124, wherein the security association comprises:

one or more alternative security protocols.